

# Analysis of Invulnerability of China Railway Express Logistics Network Based on Node Importance

Wang Nana\*, Shao Kaixuan

School of Liberal Education, Liaoning University of International Business and Economics, Dalian, China

## Email address:

wangnana124@aliyun.com (Wang Nana), 37220600@qq.com (Shao Kaixuan)

\*Corresponding author

## To cite this article:

Wang Nana, Shao Kaixuan. Analysis of Invulnerability of China Railway Express Logistics Network Based on Node Importance. *Science Discovery*. Vol. 10, No. 2, 2022, pp. 88-91. doi: 10.11648/j.sd.20221002.22

Received: March 13, 2022; Accepted: May 2, 2022; Published: May 12, 2022

**Abstract:** In order to study the weak links of the China-Europe freight train logistics network, the countries and cities along the route are counted, and the China-Europe freight train container logistics network is constructed, and a node importance analysis method is designed by combining the node degree and betweenness of the network. In this paper, random attack and deliberate attack are used to study the changes of network characteristic values, such as the average degree of the network, the proportion of isolated nodes, the average path length, and the network efficiency. The research shows that under the deliberate attack, the node average degree, aggregation coefficient, network efficiency, and average path length of the China-Europe train network decrease rapidly with the increase of the attack ratio and decrease to 0. Under random attack, the average node degree, network efficiency, and average path length of the network show a slow decrease trend with the increase of the attack ratio, and the aggregation coefficient shows a trend of slow increase and then decrease. The isolated node is no longer connected to other nodes under the deliberate attack and random attack, so the attacked node is the isolated point, which increases the cardinality of the isolated node. The China Railway Express network is relatively strong under random attacks, and relatively vulnerable when it is deliberately attacked. It is found that some nodes in the China Railway Express play an important role in the connectivity of the network.

**Keywords:** China Railway Express, Complex Network, Vulnerability

## 基于节点重要度的中欧班列物流网络抗毁性分析

王娜娜\*, 邵凯旋

辽宁对外经贸学院通识教育学院, 大连, 中国

## 邮箱

wangnana124@aliyun.com (王娜娜), 37220600@qq.com (邵凯旋)

**摘要:** 为研究中欧班列物流网络的薄弱环节, 对沿线途径国家和城市进行了统计, 构建中欧班列集装箱物流网络, 将网络的节点度和介数相结合设计了一种节点重要度分析方法, 本文采用随机攻击和蓄意攻击两种攻击方式, 分别对网络的平均度、孤立节点比例、平均路径长度、网络效率等反应网络特征值的变化来研究。研究表明在蓄意攻击下, 中欧班列网络的节点平均度、聚集系数、网络效率、平均路径长度随着攻击比例的增加急速降低并且降低为0。在随机攻击下, 网络的节点平均度、网络效率、平均路径长度随着攻击比例的增加而呈现缓慢减少趋势, 聚集系数出现缓慢增加再减小的趋势。孤立节点在蓄意攻击和随机攻击下不再和其他节点连接, 因而受攻击的节点即为孤立点, 进而增加了孤立节点的基数。中欧班列网络在受到随机攻击表现的较为强壮, 在受到蓄意攻击时相对较为脆弱, 发现中欧班列中的部分节点对网络的连通性起着重要的作用。

**关键词：**中欧班列，复杂网络，抗毁性

## 1. 引言

随着现实生活中的复杂网络的结构日益增长，网络一旦遭受攻击，造成的伤害将是难以估计的，因此如何准确的预测和辨别网络脆弱环节，对网络关键部位起到指导意义。

Albret最早在2000年研究复杂网络的抗毁性，主要关注拓扑结构对复杂网络抗毁性的影响，得出网络对有目标的攻击具有很强的抗毁性[1]。

文献将节点度数和节点介数相结合提出了一种基于节点重要度的方法来研究复杂网络脆弱性的问题，并将网络效率作为衡量网络性能的指标，仿真结果显示该方法更准确的预测网络的薄弱环节[2]。

文献采用高度数、高介数等对交通网络和电力网络进行蓄意攻击，然后分析网络的各项指标的变化大小来确定各部分的脆弱程度[3-6]。

吴迪针对海上丝绸之路集装箱海运网络的脆弱性问题[7]，构建了丝路网路，并运用复杂网络理论对丝路网络进行网络结构分析，采用随机攻击和蓄意攻击两种攻击方式分析网络连通性的特值的变化，并指出哪些地区是攻击性薄弱的地区，并提出相应的对策，很有应用价值。

文献研究对恐怖袭击背景下港口安全的可靠性进行了分析[8-11]。

许英明针对中欧班列通而不畅，即两端快、中间慢的运输状况，提出了共同发力的对策，提高通行效率，完善一带一路的通道通畅[12]。

吴珊等针对网络的脆弱性对航运贸易的影响的问题，运用复杂网络的理论与方法探究全球海运网络的脆弱性，研究表明蓄意攻击比随机攻击下网络的脆弱性表现更明显，网络效率下降速度更快[13]。

王诺针对全球集装箱海运网络脆弱性的变化趋势，运用复杂网络理论提出网络压力测试方法，以2004年和2014年为例按照节点度大小以1%-10%的比例逐渐删除节点和对应的边，分析量化指标的变化，研究成果对深化港口地理研究有借鉴作用[14]。

计明军等在一带一路的倡议下，针对新亚欧大陆桥运输的中欧班列的特殊性，分析物流园区存在的问题，提出了不同物流节点建设差异化的物流园区，加强物流园区的合作，从而促进新亚欧大陆的畅通运行[15]。

上述网络分析方法用高度数或者高介数进行网络攻击时存在一定的单因素影响，不能准确的反映网络各部位的脆弱程度，有的节点低介数可能具有很高的度数，该节点受到攻击时网络结构会发生变化，进而影响整个系统的运行，因此本文提出一种将度数和介数相结合的方法，将两者进行非线性归一化处理作为节点的重要度值。

## 2. 网络构建

中欧班列是按照固定车次、固定线路、固定班期和全程时刻表开行，运行中国与欧洲以及一带一路沿线国家

间的集装箱等铁路国际联运列车。中欧班列已形成三大通道、四大口岸、五个方向、六大线路为特点的基本格局。研究中欧班列网络的脆弱性，找到网络的薄弱环节，对沿线国家的贸易合作具有重要意义。

本文统计63条中欧的班列信息，每条班列包括出发点、到达点、出境城市、途径国家或者城市。

中欧班列网络模型构建方式如下：

(1) 每个城市为1个节点。

(2) 城市之间的运输是往返的，因此不考虑边的方向，将网络抽象为无向网络。

### 2.1. 网络平均节点度

网络平均度的概念指的是网络中所有节点的节点度的平均值，当中欧班列的主通道遭受攻击时即网络中所有节点的节点度平均值。实际中，当网络主通道遭受攻击时，网络的节点和边也随着减少，网络节点的平均度也随着变化，平均度变化率越大说明网络越敏感也就是意味着越脆弱，设  $N$  为中欧班列网络的节点总数， $K$  为中欧班列网络的平均度， $k_i$  为节点  $i$  的节点度，则

$$K = \frac{1}{N} \sum_{i=1}^N k_i \quad (1)$$

### 2.2. 孤立节点比例

孤立节点即没有边与其相连接的节点所占的比例。当网络中的站点因遭受攻击而导致网络运输无法正常运营时，进而影响整个网络的规模和连通性，则孤立节点变化比例为：

$$\Delta N = \left(1 - \frac{N^*}{N}\right) \times 100\% \quad (2)$$

### 2.3. 平均路径长度

平均路径长度指的是网络所有节点对之间最短路径的平均值，它也是一项衡量网络脆弱性的重要指标。一般情况下，在网络遭受攻击时，但网络还没有导致网络支离破碎，平均路径长度能够反映节点间的平均分离程度，设  $d_{ij}$  为节点  $i$  和节点  $j$  之间最短路径长度，即网络平均路径长度  $L$  的计算公式为：

$$L = \frac{2}{N(N-1)} \sum_{i=1}^N \sum_{j=i+1}^N d_{ij} \quad (3)$$

### 2.4. 网络效率

网络效率指的是所有节点效率的总和，它反映的是网络运输的难易程度，网络效率越高说明网络的连通性越好，设  $h_{ij}$  为距离  $d_{ij}$  的倒数， $E$  为网络效率，则

$$E = \frac{1}{N(N-1)} \sum_{j=1}^N \sum_{i=1(i \neq j)}^N h_{ij} \quad (4)$$

2.5. 聚集系数

聚集系数指的是在网络中连接同一个节点的两个节点之间连接的平均概率,它反映了网络的聚集程度。当网络中的节点遭受攻击时,网络就会变得松散,从而网络的聚集系数也就下降,设节点的聚集系数:

$$C_i = \frac{2M_i}{k_i(k_i-1)}, i=1,2,3,\cdots,N$$
 (5)

公式(5)中:  $M_i$  为节点  $i$  的相邻节点间存在的边数。  
网络的聚集系数  $C$  的计算公式如下:

$$C = \frac{1}{N} \sum_{i=1}^N C_i$$

2.6. 节点重要度

将节点的度数和节点的介数进行归一化处理,

$$I_i = b_i + \sqrt{a_i}$$
 (6)

其中,  $a_i$  为节点的度数归一化数值,  $b_i$  为节点  $i$  的介数的归一化。

3. 网络节点脆弱性分析

蓄意攻击和随机攻击是检验网络脆弱性的主要方式,随机攻击指的是以一定的概率对网络节点进行删除,来模拟随机事件对中欧班列造成的影响。蓄意攻击指的是对网络中节点按照节点度从大到小依次删除来研究对中欧班列影响。为了量化网络的脆弱性,本文逐步以1.3%的比例模拟随机攻击和蓄意攻击,统计网络在遭受攻击时平均节点度、聚集系数、孤立节点比例、网络效率、平均路径长度等网络特征的变化。

从以下图1-5可以看出,网络在遭受随机攻击时,网络的平均节点度、聚集系数、孤立节点比例、网络效率、平均路径长度的变化幅度较为缓慢。网络在遭受蓄意攻击时,网络的平均节点度、聚集系数、孤立节点比例、网络效率、平均路径长度变化幅度较大,这说明网络在遭受随机攻击时,表现的较为强壮。网络在遭受蓄意攻击时,表现的较为脆弱。

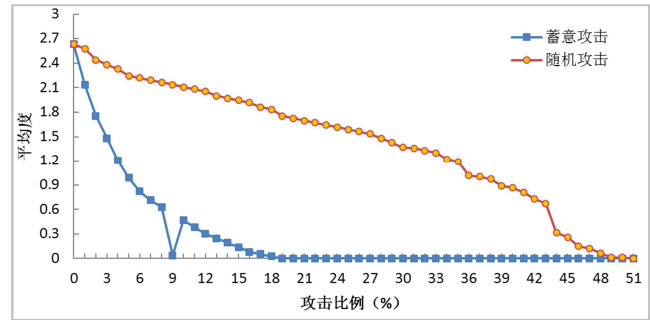


图1 网络平均度。

从以下图1可以看出,网络在遭受随机攻击时,网络的平均节点度变化幅度较为缓慢。网络在遭受蓄意攻击时,网络的平均节点度变化幅度较大。

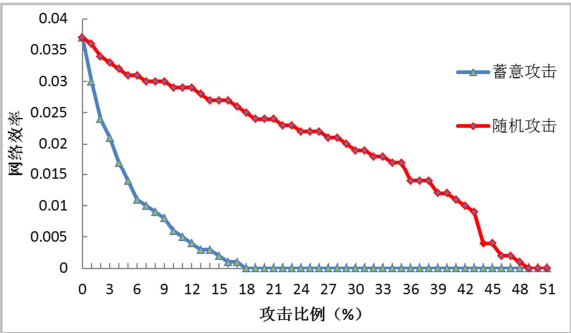


图2 网络效率。

从上图2可以看出,网络在遭受随机攻击时,网络的网络效率的变化幅度较为缓慢。网络在遭受蓄意攻击时,网络的网络效率变化幅度较大,攻击比例在18%时,网络的网络密度为零。

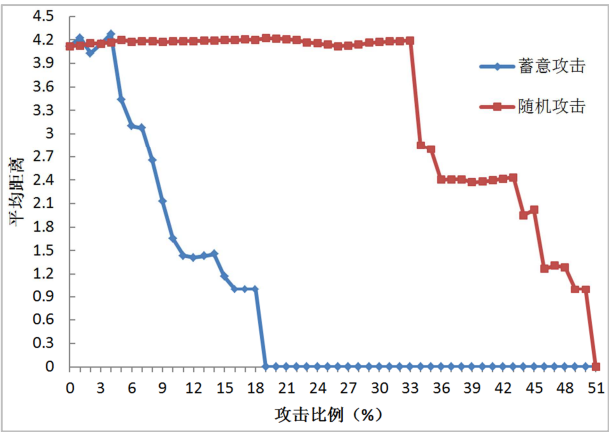


图3 平均距离。

从上图3可以看出,网络在遭受随机攻击时,平均路径长度开始变化不大,在攻击比例为33%时,出现大幅度下降。网络在遭受蓄意攻击时,网络的平均路径长度变化幅度较大。

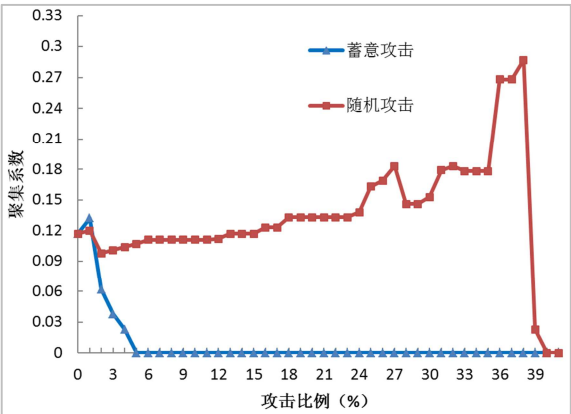


图4 聚集系数。

从上图4可以看出,网络在遭受随机攻击时,网络的聚集系数的变化幅度开始较为缓慢,在攻击比例达到37%时出现急速下降。网络在遭受蓄意攻击时,网络的聚集系数变化幅度较大,在攻击比例达到5%时,聚集系数为零。

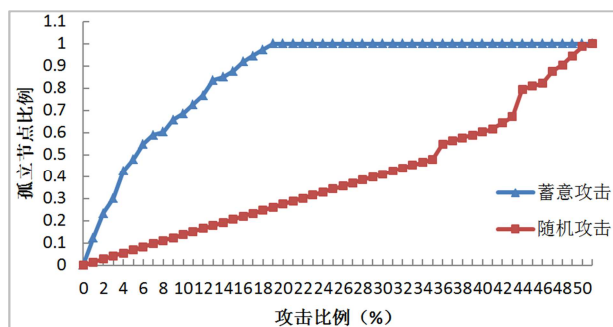


图5 孤立节点比例。

从上图5可以看出,网络在遭受随机攻击时,网络的孤立节点比例的变化幅度较为缓慢。网络在遭受蓄意攻击时,网络的聚集系数变化幅度较大,在攻击比例达到20%时,网络基本上是零散状态。

从上图可以看出,在蓄意攻击下,中欧班列网络的节点平均度、聚集系数、网络效率、平均路径长度随着攻击比例的增加急速降低并且降低为0。在随机攻击下,网络的节点平均度、网络效率、平均路径长度随着攻击比例的增加而呈现缓慢减少趋势,聚集系数出现缓慢增加再减小的趋势。孤立节点在蓄意攻击和随机攻击下不再和其他节点连接,因而受攻击的节点即为孤立点,进而增加了孤立节点的基数。

#### 4. 结论

本文统计中欧班列的运营线路,利用复杂网络理论研究中欧班列的脆弱性,构建中欧班列集装箱物流网络,将网络的节点度和介数相结合设计了一种节点重要度得分分析方法,本文采用随机攻击和蓄意攻击两种攻击方式研究表明网络的脆弱性,在蓄意攻击下,中欧班列网络的节点平均度、聚集系数、网络效率、平均路径长度随着攻击比例的增加急速降低并且降低为0。在随机攻击下,网络的节点平均度、网络效率、平均路径长度随着攻击比例的增加而呈现缓慢减少趋势,聚集系数出现缓慢增加再减小的趋势。研究表明,在随机攻击下相对较为强壮,在蓄意攻击下网络较为脆弱,同时中欧班列中的部分节点对网络的连通性起着重要的作用。

#### 致谢

本文为辽宁对外经贸学院校级课题博士科研启动基金(2021XJLXBSJJ03)的阶段性成果之一。

#### 参考文献

- [1] Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex networks [J]. Nature, 2000, 406: 378-382.
- [2] DUAN Jiarong, ZHENG Hongda. Vulnerability analysis method for complex networks based on node importance [J]. Control Engineering of China, 2020, 27 (4): 692-696.
- [3] Zhao S C. Study on Reliability of Urban Public Transit Network Based on Complex Network Theory[J]. China Safety Science Journal, 2013, 23 (4): 108-112.
- [4] Huang D R, Shen L B, Zhao L. Vulnerability Analysis of Urban Road Network Based on Complex Network Theory [J]. Journal of Chongqing Jiaotong University (Natural Science), 2015, 34 (1): 110-115.
- [5] Liu D C, Ji X P, Wang B, et al. Topological Vulnerability Analysis and Countermeasures of Electrical Communication Network Based on Complex Network Theory[J]. Power System Technology, 2015, 39 (12): 3615-3621.
- [6] Jiang X Y, Ji X, Huang J. Vulnerability Analysis of Shipboard Power Network Based on Complex Network Theory[J]. Ship Science and Technology, 2014, (8): 46-52.
- [7] WU Di, WANG Nuo, YU Anqi, GUAN Lei. Vulnerability and risk management in the maritime silk road container shipping network [J]. Acta Geographica Sinica. 2018, 73 (6): 1133-1148.
- [8] Yang Z L, Adolf N, Wang J. A new risk quantification approach in port facility security assessment [J]. Transportation Research Part A, 2014, 59: 72-90.
- [9] Yang Z L, Adolf N, Wang J. Prioritising security vulnerabilities in ports[J]. International Journal of Shipping and TransportLogistics, 2013, 5 (6): 622-636.
- [10] Talas R, Menachof D. Using portfolio optimisation to calculate the efficient relationship between maritime port security residual risk and security investment[J]. International Journal of Shipping and Transport Logistics, 2014, 6(3): 314-338.
- [11] Germond B. The geopolitical dimension of maritime security [J]. Marine Policy, 2015, 54: 137-142.
- [12] 许英明, 刑李志, 董现奎. 一带一路倡议下中欧班列贸易通道研究[J]. 国际贸易, 2019, 2: 80-86.
- [13] 吴姗, 韩晓光, 刘姗姗等. 基于复杂网络的全球海运网络脆弱性分析[J]. 计算机工程与应用, 2018, 54 (15): 249-254.
- [14] 王诺, 董玲玲, 吴暖, 颜华锟. 蓄意攻击下全球集装箱海运网络脆弱性变化[J]. 地理学报, 2016, 71 (2): 293-303.
- [15] 计明军, 刘双福, 郭兴海. 新亚欧大陆桥沿线物流园区发展规划研究[J]. 铁道运输与经济, 2019, 41 (2): 94-99.